	Montana Operations Manual ***STANDARD TEMPLATE***	Category	Information Technology
		Effective Date	TBD
		Last Revised	
Issuing Authority	**Department of Administration** **State Information Technology Services Division**		
STD–Enterprise Infrastructure Disaster Recovery Testing			

I. Purpose

A. The purpose of this standard is to establish an enterprise method for disaster recovery testing for Enterprise Infrastructure that addresses both agency business requirements, prerequisites, preparation and expectations for disaster recovery testing. Disaster Recovery Plan according to NIST is a written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities.

II. Scope

A. This standard applies to all state agencies that use Enterprise Infrastructure hosted by SITSD. The scope includes Virtualization Services, Storage Services, Mainframe Services, Network Services, and the supporting infrastructure for these services.

III. Standard Statement

A. To support virtualization and storage disaster recovery testing, this standard requires that SITSD shall:

i. Implement and maintain VMWare Site Recovery Manager (SRM) recovery policies that specify how different virtual servers should be recovered.

Note to agencies: SITSD will provide agencies with a choice between high and low recovery priority options typically associated with production and development or test. This option is presented to the agency when they order the server. The priority establishes the order in which virtual servers are made available in the disaster recovery data center. Agencies are responsible for choosing the appropriate priority of disaster recovery that matches the business purpose of the agency assigned virtual server.

ii. SITSD shall conduct disaster recovery test no less than semiannually by using an isolated temporary copy of the

replicated data in a way that does not disrupt ongoing operations of either the Helena State of Montana Data Center (SMDC) or the Miles City Data Center (MCDC). Test will replicate data from SMDC to MCDC, and then test that the hardware, storage and replicated data successfully reports back to the VMWare Site Recovery Manager as operational within the isolated environment.

1. SITSD will submit change requests prior to the test to ensure agencies are notified.

iii. SITSD shall provide a VM Recovery Plan History Report of the disaster recovery tests that will be based from the agency specific virtual server environment. Any applications in the hosted environment by SITSD will be tested and verified by SITSD.

1. Agency participation in the execution of the disaster recovery testing is encouraged. Agencies may participate by submitting a service request that establishes their intent to participate.

B. To support mainframe disaster recovery testing, this standard requires that SITSD shall:

i. Fail over the Helena Data Center Mainframe Services to the Miles City Data Center no less than biennially.

ii. Coordinate acceptable times and duration of testing with agencies that consume mainframe services.

iii. Submit change request prior to test to ensure agencies are notified.

C. Agencies that need more in-depth testing must:

1. Submit a service request thirty (30) days in advance for disaster recovery testing that exceeds the standard.
   a. The requesting organization must submit with the service request a disaster recovery testing plan (based on a template from SITSD) which identifies the scope of the test, goals, objectives, and identified SITSD systems or services that directly link to the information system being tested.
   b. The service request must include a billing client as SITSD expert time charges may apply.
2. Upon review of the testing request and plans, SITSD may have additional requirements or processes that must be completed by the requesting organization before the test may occur. SITSD shall obtain prior customer approval of any applicable charges that may apply based on the testing request and plans

3. If agency does not require assistance from SITSD staff, the agency must open a service request with SITSD seven (7) days prior to disaster recovery testing. The service request must include the proposed dates and times of testing.

D. Outside Organizations
Organizations not associated with the State of Montana must notify the Data Center Manager by submitting a service request to servicedesk@mt.gov thirty (30) days in advance of any planned disaster recovery testing. The notification must include the proposed dates and times of testing.

E. All agencies and outside organizations are strongly encouraged to conduct a table-top exercise pertaining to the disaster recovery of the information system being tested prior to the "live" test, to help identify any logistical problems (such as licensing, personnel onsite at Miles City Data Center, etc.) or bottlenecks in processes and procedures.

F. SITSD reserves the right to block any network activity resulting from disaster recovery testing that interferes with everyday business or production network activity. Production network traffic takes precedence over disaster recovery testing traffic.

G. This Disaster Recovery Standard does not replace backups. For the VM infrastructure, only 5 days of snapshots are kept. Each state agency should have proper backups for its systems.

IV. Definitions

A. Refer to the MOM GDE-Statewide Glossary: Information Systems Policies and Standards for a list of standard definitions and to the NIST Information Security Glossary of Key Information Security Terms.
B. Backup - A copy of files and programs made to facilitate recovery, if necessary. This definition is according to NIST glossary reference above.
C. Business Continuity Plan (BCP) - The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business functions will be sustained during and after a significant disruption. This definition is according to NIST glossary reference above.
D. Disaster Recovery Plan (DRP) - A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities. This definition is according to NIST glossary reference above.
E. VMware Site Recovery Manager (SRM): is a business continuity and disaster recovery solution that helps you to plan, test, and run the

recovery of virtual machines between a protected vCenter Server site and a recovery vCenter Server site.

V. References

A. Legislation (MCA)

1. Section 2-15-112, MCA
2. Section 2-17-505, MCA
3. Section 2-17-512, MCA
4. Section 2-17-514, MCA
5. Section 2-17-516, MCA
   Section 2-17-546, MCA
6. Sections 2-17-504 et seq., MCA

B. Policies, Directives, Regulations, Rules, Procedures, and Memoranda

1. SITSD Policy: POL-Contingency Planning Policy
2. SITSD Procedure: PRO-IT Policies, Standards, Procedures and White Papers Procedure
3. POL-SITSD Leadership Roles and Responsibilities Policy
4. Administrative Rules of Montana (ARM): ARM 2.12
5. NIST: Glossary of Key Information Security Terms
6. Statewide Policy: Discipline Policy
7. Statewide Policy: Information Security Policy: Appendix B (Security Roles and Responsibilities)
8. Statewide Procedure: Action and Exception Request Procedure
9. Statewide Procedure: Establishing and Implementing Statewide IT Policies, Standards, and Procedures
10. State of Montana Office of the Governor Executive Order No. 09-2016